A publication of the DCIS Northeast Field Office

TECHNOBABBLE

The DCIS Cyber Crime Newsletter

TECHNOBABBLE
Volume 1, Issue 1

November, 2000

This issues suggested computer crime bookmarks:

National Infrastructure Protection Center:
http://www.nipc.gov

U.S. Department of Justice Cyber Crime Page:
http://www.cybercrime.gov

Tech TVs Cyber Crime Page:
http://www.techtv.com/cybercrime

Inside this issue:

Juvenile Hacker Sentenced to Jail Time

On September 21, 2000, a 16 year old computer hacker from Miami, Florida was sentenced to six months in a detention facility after pleading guilty to to acts of juvenile delinquency. This case marks the first time a juvenile computer hacker has been sentenced to serve time.

The 16 year old, known throughout the hacker community as C0mrade, admitted to illegally accessing U.S. Department of Defense and NASA computer systems.

As part of the illegal access, the juvenile obtained and downloaded information, e-mails, and proprietary software from DOD and NASA. NASA indicated that the hacker obtained information valued at approximately $1.7 million. Software illegally obtained from NASA supported the International Space Station's physical environment, including control of the temperature and humidity of the living space. The juvenile's intrusion into NASA computer systems required the systems be shut down, which caused delivery delays of the program software. This resulted in additional costs of $41,000 in contractor labor and computer equipment replacement costs.

The juvenile was also responsible for computer intrusions involving a Department of Defense computer network.

He illegally obtained more than 3,300 electronic messages, and 19 user names and passwords.

Special Agents of the Defense Criminal Investigative Service and NASA's Office of Inspector General conducted the investigation.

FBI Stresses need for Cyber Ethics Education

The FBI and the Information Technology Association of America have formed the Cybercitizen Partnership to encourage educators and parents to discuss cyber ethics with children.

According to Michael Vatis, director of the FBI's National Infrastructure Protection Center, ``One of the most important ways of reducing crime is trying to teach ethics and morality to our kids. That same principle needs to apply to the cyber world."

A recent survey found that many students in elementary and middle school don't consider hacking and other computer crimes illegal. The program attempts to inform students of the damages that hacking and other computer crimes cause, and discusses the consequences of computer crime- including potential criminal charges, impact upon private and public institutions, and resources it drains from law enforcement.

Windows NT is currently one of the most widely utilized operating systems in existence. Unfortunately, the mainstream appeal of NT has made the operating system a constant target of hackers.

While the hacking community thrives upon pointing out Windows NT security deficiencies, the truth is that Windows NT can actually be more secure than many operating systems if capable system administrators work to 'harden' NT based networks. Unlike many Unix based OS developers, Microsoft has steadfastly guarded NT source code, thus prohibiting hackers from scrutinizing the code for weaknesses and errors that could be taken advantage of. Microsoft has also been quick to patch security flaws upon discovery.

Unfortunately, many NT system administrators simply don't have the time, or haven't taken the time, to research NT security issues. The three most common issues that have caused lapses in NT system security are:

1) **Failure to keep NT Service Packs up to date.** Microsoft periodically releases "service packs" which incorporate system patches, including many security fixes. All too often, investigators find that system administrators have not installed the latest service pack. In order to ascertain whether or not your NT system has the latest service pack installed, shut down and re-boot your system. After completing POST operations, and displaying your OS loader options, a blue Windows NT boot screen will appear which will indicate the last service pack installed. As of this date, the latest service pack available from Microsoft is NT Service Pack 6a. If your system is not up to date, make sure that you obtain and install the latest service pack as soon as possible.

2) **Failure to protect Administrator accounts.** Generally speaking, hackers can do very little to a Windows NT system unless they obtain Administrator-equivalent privileges. In order to protect these accounts, system administrators need to

a) Rename administrator accounts so as to protect them from brute force password guessing attacks. In order for a hacker to gain administrator level access, he generally needs a user name/password pair. Why give a hacker half of the puzzle by failing to rename the default administrator account, or naming subsequently created accounts in a manner that reveals privilege levels?

b) Complex and lengthy administrator passwords should be utilized which employ random characters and numbers.

c) Severely limit the number of administrator level accounts available on any given system. Too many organizations provide administrator level privileges to far too many individuals. While it is undoubtedly convenient to allow multiple persons the ability to troubleshoot network problems, create user accounts, etc., the security risks inherent in assigning numerous administrator accounts far outweighs the advantages.

3) **Failure to enable security logging and audit results.** NT allows administrators to utilize the User Manager Utility to implement security logging policies. Best possible scenario is to audit all events, however, many administrators do not wish to enable all available logging. At a minimum, make sure to audit Logon/Logoff successes and failures, Use of User Rights failures, and Security Policy Changes successes and failures. Make sure your organization routinely utilizes the NT Event Viewer utility to audit critical security events (such as Login/Logoff failures). If your Event Viewer logs contain information too voluminous to sift through, utilize built in filtering abilities to help isolate useful information. For example, filtering on

"...the truth is that Windows NT can actually be more secure than many operating systems..."

event codes 529 (Logon/Logoff failure) and 539 (account locked out) can reveal unsuccessful intrusion attempts. If a series of unsuccessful attempts is immediately followed by a successful logon, an intruder may have successfully compromised your system.

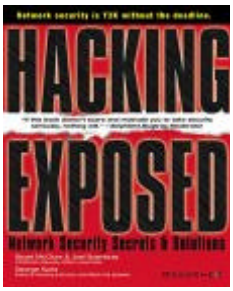
Other steps you can take to harden your system:

- Whenever possible, disable remote logins.
- Do NOT set up dual boot systems which place operating systems other than Windows NT on network hard drives. Format each hard drive using the NT File System (NTFS) option, versus FAT 32/combination OS setups.
- Regularly audit files, directories, and network nodes in order to assure that the appropriate levels of permissions/shares are assigned.
- Create a restrictive password policy that requires users to change passwords regularly, and stick to this policy.
- Disable the Last Logon user display.
- Restrict access to certain executables which users do not require.
- Physically secure your servers.
- Remove extended registry rights from the *Everyone* Group.
- Eliminate the Anonymous login (null session) vulnerabilities which allow anonymous logon users to list domain user names and enumerate share names.

Hackers who spend 20+ hours a day experimenting with operating systems in order to discover holes will undoubtedly continue to find vulnerabilities. Only Systems Administrators who diligently audit their networks, and keep their systems up to date, will successfully defend their systems from these cyber criminals.

This Issues Suggested Reading

Hacking Exposed



This issues suggested reading is "Hacking Exposed-Network Security Secrets & Solutions," (McClure et. Al). Regarded as one of the finest hacking texts available, "Hacking Exposed" discusses common methodologies utilized by hackers to penetrate computer systems. In fact, the text is so comprehensive that some internet security organizations feared its release, and questioned the authors' wisdom in explaining hacking methods in such a detailed manner. These critics complained that the book could potentially be utilized by aspiring malicious hackers as a step by step guide to infiltrating networks. In fact, the authors own words within the books introduction state that, "We really want to give people detailed instructions on how to hack computer networks in plain, uncomplicated terms." (Introduction, p. xxiii). However, the authors go on to explain that the only truly effective manner of defeating hackers is to learn their methods, and to expose the holes they regularly utilize to illegally access systems.

Regardless of your opinion as to whether a text should provide step by step instructions for compromising a computer system, "Hacking Exposed" is a must read for any individuals who have network security functions, or for those who investigate computer compromises. The text contains information relative to vulnerabilities within the most common operating systems (Windows 95/98, Windows NT, Unix based systems, and Novell Netware based systems), and upon exploring these holes, provides countermeasure information.

Title:
Hacking Exposed: Network Security Secrets & Solutions.

Authors:
McClure, Scambray & Kurtz

Cost: **$39.99**

ISBN: **0-07-212127-0**

Publisher: **Osborne/McGraw Hill**

This Issue's Useful Definition

Ports

Once you begin to explore the world of Internet crime, you will undoubtedly hear the phrase "port" time and time again. Perhaps you have heard system administrators reference the fact that their systems have been the target of numerous "port scans." So what are ports, and why are they so important?

In addressing students that are relatively new to the world of computers, many instructors define ports as entry and exit points into a computer system. Unfortunately, this definition is not at all accurate. In reality, ports are better defined as **unique numbers assigned to services which are present on a given computer system**.

In order for computers within a network to communicate, they must use a standard language, known as a protocol. Computers connected to the Internet utilize a protocol suite known as TCP/IP (Transmission Control Protocol/Internet Protocol) which allows the systems to communicate regardless of hardware and operating system differences. It is for this reason that Microsoft Windows computers and Unix based computers can communicate via the Internet regardless of the fact that the respective operating systems are very different.

TCP/IP must continually manage multiple services in order to allow computers to communicate. For example, TCP/IP utilizes a service known as Simple Mail Transfer Protocol (SMTP) to manage e-mail, File Transfer Protocol (FTP) to allow direct transfer of files between computers, the Telnet service to allow direct, remote connection to another computer, and the Hyper Text Transfer Protocol (HTTP) to allow world wide web based communication. In an attempt to manage these services, TCP/IP assigns a unique number, called a *port number*, to each service. Common known protocols have well known port numbers. For example, HTTP is generally assigned a port number of 80, while SMTP is generally assigned a port number of 25.

When a specific service is, in fact, active on a given system, that port is said to be "active", or "listening." For example, a system which functions solely as a mail server would most likely be listening for a SMTP connection on port 25, but would not (or at least should not) be listening for a HTTP connection on port 80 since the computer is not functioning as a web server.

So if ports are simply numbers, why are they so important to computer crime investigators? The answer lies in the fact that **active ports reveal information about a given computer system, thus exposing potential vulnerabilities.** Hackers take advantage of the fact that computers **must** listen on a port in order to communicate with other systems. They use readily available software packages known as "port scanners" to ascertain what services are active on a computer. For example, lets say a hacker uses a scanner, and determines that a certain system is "listening" on port 25 utilizing an older version of SMTP. The hacker can then consult any number of well known web sites in order to research whether the version of SMTP which is active on the computer has vulnerabilities or weaknesses that make the system prone to compromise. Utilization of port scanners in this manner is generally one of the first stages of a hacker's quest to break into a system. The process is generally known as the **footprinting, or reconnaissance** stage of an attack, since the attacker gathers information without actively utilizing attack methodologies.

Unfortunately, all too often system administrators leave applications active which should be disabled. For example, it is not at all uncommon to find mail servers with an active HTTP connection on port 80, or web servers which allow active telnet connections via port 23. When ports are active which should be disabled, they offer a would-be intruder one more avenue to explore in his quest to attack a system.

> *"In reality, ports are better defined as unique numbers assigned to services which are present on a given computer system."*

Commonly Utilized Port Numbers

Port	Service
21	File Transfer Protocol
23	Telnet Protocol
25	Simple Mail Transfer Protocol
53	Domain Name Service
69	Trivial File Transfer Protocol
79	Finger Protocol
80	Hyper Text Transfer Protocol
6665 to 7000	Internet Relay Chat

PGP Vulnerability Identified

Recently, a vulnerability in Pretty Good Privacy (PGP) has been widely discussed in the information security community. Certain versions of PGP software don't automatically check to see if the Additional Decryption Key (ADK) has been signed, altered, or appended. A moderately to highly skilled attacker could exploit the contents of a victim's PGP-encrypted communications if the following conditions are met: (1) the attacker has access to the victim's key, (2) the attacker alters and propagates the victim's key, and (3) the attacker has access to victim's email encrypted with the altered key. This vulnerability only provides access to the encrypted contents of PGP message provided all three of these prior conditions are already met.

Using this vulnerability, an attacker can insert his own key into any valid certificate. What this means is that an attacker can take a PGP certificate, append his own key to the victim's valid certificate as an ADK, and spread it out to the world. This tampered version of the certificate will remain unnoticed by anyone using affected versions of PGP who doesn't manually examine the bytes, and anyone using that tampered version will automatically and invisibly encrypt all messages to the attacker as well as the certificate owner.

The encryption software industry has identified a solution for this vulnerability and will be releasing a patch. A full description of the vulnerability can be found at:

http://www.cert.org/advisories/CA-2000-18.html

New Variants of Trinity Discovered

New variants of the Trinity and Stacheldraht Distributed Denial of Service (DDoS) tools have been found in the wild. As was demonstrated in February of this year, DDoS attacks can bring down networks by flooding target machines with more traffic than the machines can process. It has recently been determined that masters tied to zombies have been placed on many users' systems, heightening the possibility of a DDoS attack in the future. In addition to large corporate and university systems, affected users also include those with home computers having broadband access such as DSL and cable modem. The NIPC has recommends that all computer network owners and organizations examine their systems for evidence of DDoS tools, including Trinity and Stacheldraht.

The "Trinity v3" Distributed Denial of Service (DDoS) exploit represents a potentially serious and continuing threat to networked computers running certain versions of the Linux operating system**.** Trinity v3 is a DDoS tool that is controlled via IRC or ICQ. When a system has been compromised and the Trinity v3 tool installed, each compromised machine joins a specified IRC channel and waits for commands. The Trinity v3 tool enables intruders to use multiple, Internet-connected systems to launch packet flooding denial of service attacks against one or more target systems. At least eight variations of Trinity have been found on the Undernet Internet Relay Chat network, each reporting to a different IRC channel. Trinity v3 responds to bTrinity responds to lines beginning with "(entitee)."

System administrators should Trinity portshell installed. Trinity v3 is difficult to detect because the agent does not listen to specific ports to receive commands, but receives them over IRC. Watching for suspicious IRC traffic is useful in detecting Trinity v3. It is important to note that if Trinity v3 is found on a system, the system may have experienced root level compromise.

NIPC's DDoS detection tool has been modified to detect Trinity v3 and some new variants of Stacheldraht. While the tool is designed to detect mutations of these DDoS tools, it may not detect all variants of the tools. NIPC reports that it will continue to update the detection tool as we receive new DDoS variants. For more info, refer to

http://www.nipc.gov/warnings/alerts/1999/trinoo.htm

As was demonstrated in February of this year, DDoS attacks can bring down networks by flooding target machines with more traffic than the machines can process.

A publication of the DCIS Northeast Field Office

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: Jives@dodig.osd.mil

We're on the Web!
www.dodig.osd.mil/dcis/dcismain.html

The Defense Criminal Investigative Service

"Protecting America's War Fighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, export enforcement violations, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.
10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency
Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency
525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency
Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency
One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty
1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency
441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099